EXHIBIT E

AirDefense

Release Notes r3.0

The following are release notes for AirDefense Release 3.0.

Full documentation is online!!! See the Help Menu in the AirDefense Server graphical user interface.

New Features

AirDefense Release 3.0 has new features in the AirDefense Server Graphical User Interface (GUI), the Command Line Interface, and the AirDefense Sensor User Interface (UI).

AirDefense GUI

The AirDefense GUI for Release 3.0 has the following new features.

All Program Areas

- Color-coded icons now display throughout the AirDefense GUI, in both the information screen displays and tables, and in structured "trees" that provide a hierarchal approach to managing devices. There are *static* icons and *stateful* icons. Static icons represent the System, and the Locations and Groups of Sensors. Stateful icons represent the presence, associations, and states of individual Sensors, Access Points, and Stations in your wireless local area network (WLAN).
  - — Icons identify network elements and their associations in the network.
  - — Colors identify the state of each network element.
- Access Points can now display as a MAC address, an IP address, a user-defined name, or a DNS name; Stations can now display as a MAC address, an IP address, a user-defined name, a DNS name, or a LEAP name. Sensors can now display as a MAC address, an IP address, or a user-defined name. You can select this in Administration.

Dashboard

- Dashboard now displays the color-coded icons for easy identification of Sensors, Access Points, and Stations in the WLAN.
- A new Alarm Filter pull-down enables you to filter the alarms by Device, by Type, by Device and Type, or by Show Details (which includes Location, Group, and Sensor). The Recent Alarms information that displays depends on the filter you choose.

Alarm Manager

- A new **Adjust Priorities** feature enables you to change the priority of an alarm whenever you choose. An Adjust Alarm Priorities screen shows the alarm priorities, and groups alarms by classes.
- A new **Purge Cleared** feature enables you to permanently remove all cleared alarms the AirDefense database.
- A newly-designed filter field enables you to choose one of the built-in, or already configured filter settings that determines how you view alarms. Alternately, you can form your own filter, using Alarm Manager's filter editing features--Basic Alarm Filter and Advanced Alarm Filter.
- A new **Basic Alarm Filter Editor** enables you to run a basic filter. You can determine the detail level of filters (if and how alarms are summarized and which columns display); limit alarm queries to devices; and determine the time range for the report, for example, the last 24 hours.
- A new **Advanced Alarm Filter Editor** enables you do basic filter editing, and enables you to edit existing filters, add a new filter, copy a filter, or delete a filter. Filters you configure here are saved to the AirDefense database.
- A new **Notes** field enables you to add a comment next to each alarm.
- New Alarm Types:
  - — **Network Scan AirMagnet:** Occurs when the tool AirMagnet has started. While the tool is running, it is completely passive, which is why we can only see it start. Critical.

- **Network Scan Wellenreiter:** Occurs when the tool Wellenreiter has started. Wellenreiter is an open source tool that performs discovery, penetration, and auditing of 802.11b networks. Critical.
- **Roaming:** Occurs when a Station that is authorized on at least one authorized Access Point associates to another authorized Access Point, but for which the Station is not authorized. Critical.
- **Vendor Policy:** Occurs when a Station associates to an authorized Access Point, but the vendor of the wireless card does not match the Vendor Policy that is defined for that Access Point. Critical.
- **Watch List:** Occurs when a Station that has been placed on the Watch List is active in the WLAN. Critical.
- **Network Scan:** XP Protection: Occurs when a user on Windows XP is using tools provided by XP to scan the WLAN. Critical.
- **Sensor Hardware Failure:** Occurs when a Sensor hardware or firmware failure causes the Sensor to lose connection with the AirDefense Server. Critical.
- **Sensor Failed Login:** Occurs when there are three unsuccessful attempts to enter either a User Name or a Password that are not recognized by AirDefense. Critical.
- **Sensor Offline:** Occurs when the Sensor goes offline from the AirDefense Server. Critical.

Sensor Manager

- Link encryption for data between the Sensor and the AirDefense Server is now available.
- You can now configure the Sensor for a Secondary AirDefense Server IP address. If your WLAN is using more than one AirDefense Server, this gives the Sensor an alternate data path if it loses communication with the Primary AirDefense Server.

Policy Manager

- AirDefense now can detect **LEAP** and **802.1x** authorization modes for both Access Points and Stations.
- You can now place Stations on a **Watch List**. AirDefense generates an alarm when it detects a Station on the Watch List.
- You can now place Stations on an **Ignore List**. AirDefense sees, but ignores any Station or associated Access Point on this list, giving you a tool to place foreign Stations in a "friendly" status. Stations on the Ignore List do not generate alarms.
- You can now import Access Points and Stations into AirDefense using either of two methods. One method enables you to import from a ASCII comma delimited flat file with predefined format. A second method enables you to import from a Cisco Access Control Server. You can pre-authorize devices during import.
- A new Vendor policy makes it possible to ensure that only wireless cards from approved vendors are allowed to associate to Access Points in your WLAN. Wireless cards not on approved Vendor lists generate a Vendor Policy alarm.

Notification Manager

- Daily and weekly email (in html) Management Reports are now available. These coincide with the information in report summaries that display in Reports. These are: Device Summary, Device List, Policy Summary, and Health Summary.
- SNMP notifications now have filtering that allows receipt of alarms by priority (Critical, Major, and Minor). Additionally, SNMP configuration now has a field for a community string for SNMP communications.

Reports

- System Reports, which consisted of a Performance Snapshot and a Security Snapshot in Release 2.1, have been redesigned into a new Summary category, consisting of eight new reports:
  - **Device Summary:** Count of all authorized and unauthorized Access Points and Stations, and a count of all Sensors deployed on your WLAN.
  - **Device List:** Displays all devices that are currently active in your WLAN on any given date, by device and type.
  - **Missing Devices:** Displays ID information about authorized (only) Access Points and Stations that the Sensor has not been able to see for a user-configured length of time.
  - **Threat Summary:** Summarizes activities that are threatening the network: alarm summaries, network probes, and after hour activities.
  - **Policy Summary:** Summarizes policy monitoring for Access Points in your WLAN.
  - **Health Summary:** Shows a comprehensive health report on device activities, such as downtime and use statistics, noisiest channels, and frequency of use statistics for Access Points and Stations.
  - **Ad Hoc Networks:** Shows the Access Points and Stations currently engaged in ad hoc networking, by MAC address and Name, Group, Location, and Sensor.
  - **Rogue Summary:** Shows details on unauthorized Access Points and Stations in your WLAN.

- Sensor has one new report:
  - **Sensor Performance View:** Displays a daily overview of your network statistics per channel, based on selected Sensors.
- Access Point has two new reports:
  - **AP Policy Violations:** Displays information on Access Points that are in violation of policies.
  - **Unauthorized APs:** Displays all Access Points that are not authorized on the WLAN, by MAC address and Name, Group, Location, and Sensor.
- Station has one new report:
  - **Probing Stations:** Displays identification information on Stations that are probing your WLAN.

Administration

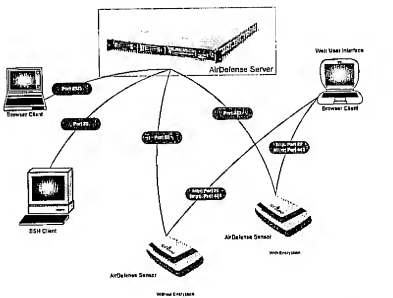
- You can now assign user access to AirDefense based on user roles–*Admin and Guest*. Admin (administrators) have complete viewing and configuration capabilities. Guests only have viewing capabilities.
- New software features give you methods to do the following on-demand or by schedule:
  - Check for software updates (AirDefense automatically downloads available updates.)
  - Export data
  - Backup data

  Refer to new Command Line Interface commands RCVRDB, BCKUPDB, and UPGRADE for data retrieval and installation.
- A new User Display Preferences feature enables you to choose names for devices and preferences for display throughout the AirDefense GUI. Access Points can now display as a MAC address, an IP address, a user-defined name, or a DNS name; Stations can now display as a MAC address, an IP address, a user-defined name, a DNS name, or a LEAP name. Sensors can now display as a MAC address, an IP address, or a user-defined name.

Sensor UI

The Sensor UI for Release 3.0 has the following new features.

- **https access is now enabled:** When configuring Sensor network settings, you can use https (SSL protocol) or http.
- **Link encryption is now available:** The Sensor can now communicate with the AirDefense Server via an encrypted link, using Port 443.
- **Settings for a Secondary AirDefense Server is now available:** You can now configure the Sensor for a Secondary AirDefense Server IP address. If your WLAN is using more than one AirDefense Server, this gives the Sensor an alternate data path if it loses communication with the Primary AirDefense Server.



AirDefense

Command Line Interface

The Command Line Interface for Release 3.0 has the following new commands. The first three commands on the list below, RCVRDB, BCKUPDB, and UPGRADE, are the commands for data retrieval and installation. For configuration and scheduling, see the new software features under Administration.

- **RCVRDB:** Recover databases. This command recovers the AirDefense database from a backup file.
- **BCKUPDB:** Backup databases. This command backs up the AirDefense database.
- **UPGRADE:** Upgrade system. This command upgrades the entire code set on the AirDefense Server to a newer version.
- **PING (enable/disable):** This command changes the ping setting for the AirDefense Server. PING is enabled by default. PING makes it possible for you to ping the AirDefense Server from a remote location, and also allows outgoing pings from the AirDefense Server to other network nodes.

Issues

The following issues are known for Release 3.0.

- **Upgrading the Sensor Firmware**--When upgrading the Sensor firmware: Firmware upgrades will not work over **https** with some combinations of Microsoft Windows and Microsoft Internet Explorer. Use **http** if necessary.
- **AirDefense GUI**
  - — Wired network gateway IP address appears in the Station list (609).
  - — In some program areas, columns may sort based on MAC address, even when the User Display Preferences feature is set to use a different Device Identifier (848).
  - — Alarms: Ad Hoc and Time-of-Day Alarm Icons may not always indicate the correct state (844).
  - — Ad Hoc and Time-of-Day Policy Alarms generate on Stations set for Ignore (959).

Bug Fixes

The following bugs from previous releases have been corrected.

- Sensor Manager
  - — Sensor Manager shows Sensors active that are not active (536).
  - — Sensors reappear in Sensor Manager after deletion (573).